Rekommendation om personuppgiftsansvar och ansvar för allmän handling i Säker digital kommunikation

Version 1.1

inera
Ett företag inom SKR

Innehåll

Innehåll

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	2022	Marco de Luca	Version baserad på Regelverk för anslutning till Säker digital kommunikation – Informationssäkerhet version 1.2 (2022)
1.1	2023-04-20	Malin Domeij	Version i ny Word-mall samt uppdaterad i enlighet med Regelverk för anslutning till Säker digital kommunikation version 1.4 (2023). - kap. 1, Inledning, tillkommit. - kap. 2 och 3, uppdaterade och kompletterade texter och illustrationer. - kap. 4, Referenser, tillkommit.

1. Inledning

Syftet med denna rekommendation är att stödja enhetlig hantering av personuppgiftsansvar och ansvar för allmän handling vid användning av Säker digital kommunikation (SDK).

Målgruppen är t.ex. dataskyddsansvariga och informationssäkerhetsansvariga hos användarorganisationer som ska införa SDK.

Rekommendationen har tagits fram av informationssäkerhetsarbetsgruppen för SDK och ska ses som ett stöd i tillämpningen av Avsnitt 3.3, Personuppgiftsansvar och ansvar för allmän handling, i Regelverk för anslutning till Säker digital kommunikation – Informationssäkerhet (hädanefter benämnt ”Regelverket”).

För information om Regelverket och IT-säkerhetsbilaga till Regelverket [1] samt definitioner [2], se tjänstens informationssida.

2. Personuppgiftsansvar vid kommunikation via SDK

2.1 Regelverket med kommentarer

I Regelverket, avsnitt 3.3.1, anges att:

Ett meddelande som innehåller personuppgifter och som överförs via SDK betraktas som personuppgift även om det är krypterat.

Kommentar: Personuppgifter kan förekomma både i meddelandetexten och i bilagor som bifogas till meddelandet.

Sändande respektive mottagande användarorganisation är personuppgiftsansvarig för de personuppgifter som hanteras i den egna organisationens lokala komponenter och accesspunkt samt för de loggar som avser användarorganisationens administration i SDKs gemensamma komponenter.

Sändande användarorganisation är personuppgiftsansvarig för de uppgifter som överförs. Ett nytt ansvar avseende fortsatt personuppgiftsbehandling uppstår hos mottagande användarorganisation. Detta sker när mottagande användarorganisations accesspunkt har skickat transportkvittens till sändande användarorganisations accesspunkt.

Kommentar: Se illustration nedan i 2.2.

SDK-federationsoperatör och Ansvarig för eDelivery transportinfrastruktur är inte part i användarorganisationers behandling av personuppgifter vid överföring av meddelanden via SDK och eDelivery transportinfrastruktur.

Kommentar: Inera och Digg är inte delaktiga i själva meddelandeöverföringen mellan användarorganisationer. Däremot behandlar Inera och Digg personuppgifter för administratörer i centrala komponenter.

Inera behandlar de personuppgifter (namn, personnummer/HSA-id och e-post) som krävs för administratörers åtkomst till SDK Adressbok respektive SDK Testklient. Vid behandlingen är användarorganisationen personuppgiftsansvarig och Inera personuppgiftsbiträde. Detta regleras i användarorganisationens avtal med Inera om tjänsten SDK.

Digg behandlar de personuppgifter (namn och personnummer) som krävs för att ge AP-operatörens administratörer åtkomst till SMP respektive Certifikatspubliceringstjänsten. Vid behandlingen är Digg personuppgiftsansvarig och AP-operatören personuppgiftsbiträde. Information om behandlingen tillhandahålls av Digg och regleras i accesspunktsoperatörs avtal med Digg.

2.2 Illustration

Figur 1 illustrerar att respektive användarorganisation är personuppgiftsansvarig för de personuppgifter som skickas respektive tas emot via SDK samt att Inera och Digg inte är part i själva informationsutbytet.

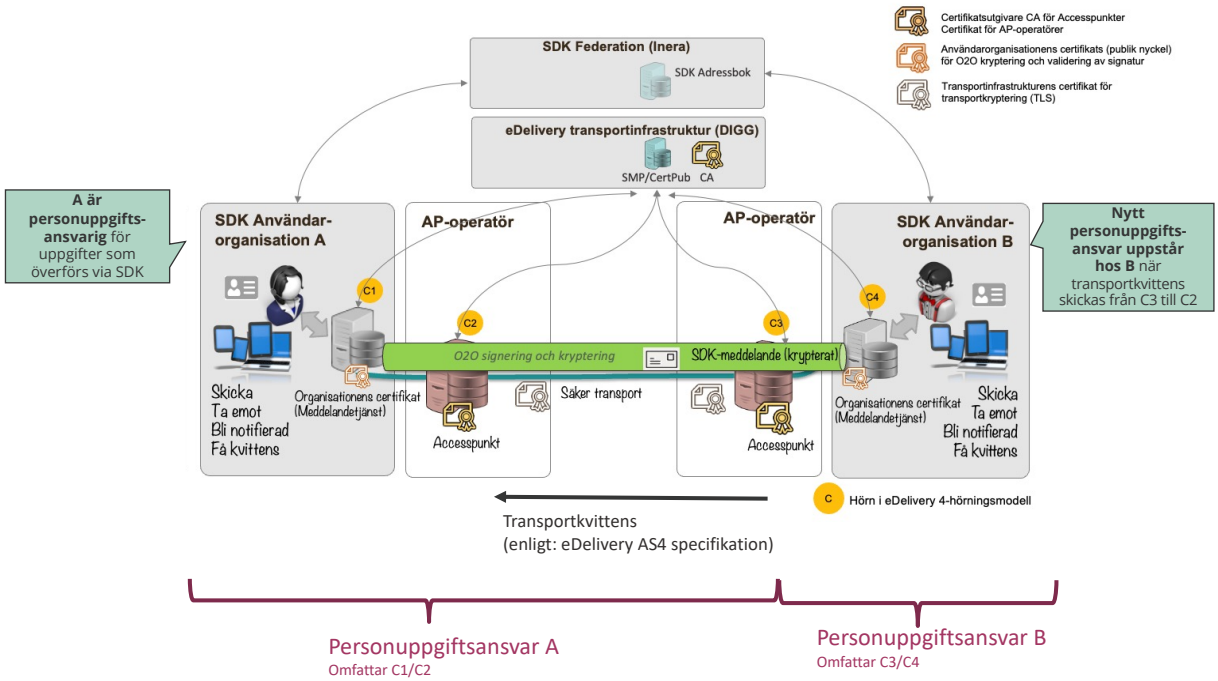
- **Personuppgiftsansvarig** för de personuppgifter som skickas och tas emot
- Ansvarar för sitt **mottagarregister** (uppgifter i SDK Adressbok)
- Ansvarig för **personuppgiftsbiträden** (t.ex. tjänsteleverantör SDK, AP-operatör)
- Ansvarar för **innehållet** och val av **kommunikationsverktyg** (anslutande system)
- Måste iaktta **externa krav** (TF, OSL, GDPR, Arkivlagen, LOU, special- eller sektoriella lagstiftningar)

*Är inte part i själva informationsutbytet men sätter upp regelverk så att **kommunikationen sker på ett säkert sätt** med lämpliga säkerhetsåtgärder*

- **Personuppgiftsansvarig** för de personuppgifter som skickas och tas emot
- Ansvarar för sitt **mottagarregister** (uppgifter i SDK Adressbok)
- Ansvarig för **personuppgiftsbiträden** (t.ex. tjänsteleverantör SDK, AP-operatör)
- Ansvarar för **innehållet** och val av **kommunikationsverktyg** (anslutande system)
- Måste iaktta **externa krav** (TF, OSL, GDPR, Arkivlagen, LOU, special- eller sektoriella lagstiftningar)

Figur 1 – Personuppgiftsansvar för information som kommuniceras via SDK

Figur 2 visar var i infrastrukturen för SDK som ett nytt ansvar avseende fortsatt personuppgiftsbehandling uppstår hos mottagande användarorganisation. Detta sker när mottagande användarorganisations accesspunkt har skickat transportkvittens till sändande användarorganisations accesspunkt.



Figur 2 – När uppstår ett nytt personuppgiftsansvar hos mottagande användarorganisation (B)

Motivering till att användarorganisation A (sändare) är ansvarig fram till att transportkvittens skickas från användarorganisation B (mottagare), är att A ansvarar för att meddelandet når rätt mottagare. Detta säkerställs genom att transportkvittens från mottagaren sänds.

3. Ansvar för allmän handling vid kommunikation via SDK

3.1 Regelverket med kommentarer

I Regelverket, 3.3.2, anges att:

Ett meddelande som överförs via SDK från en myndighet alternativt tas emot av en myndighet kan betraktas som en allmän handling enligt tryckfrihetsförordningen. Det är dock upp till varje användarorganisation att göra en egen bedömning.

- Meddelandet kan anses vara expedierat av sändande användarorganisation när det är tillgängligt för teknisk bearbetning/dekryptering hos mottagarens meddelandetjänst.
- Meddelandet kan anses vara inkommet hos mottagande användarorganisation när det är tillgängligt för teknisk bearbetning/dekryptering hos mottagarens meddelandetjänst.

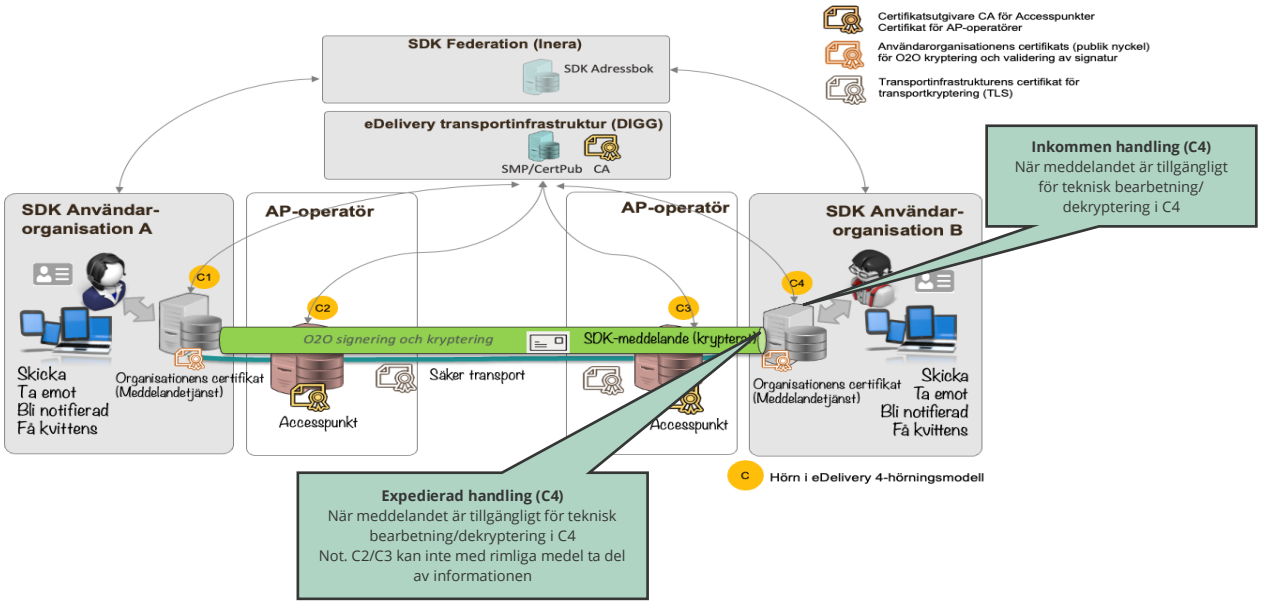
Kommentar: Se illustration nedan i 3.2.

Kommentar: Tryckfrihetsförordningen (1949:105) är tillämplig för myndigheter. Det innebär att SDKs regelverk är tillämpligt för regioner, kommuner och statliga myndigheter samt de organisationer som i övrigt tillämpar offentlighetsprincipen.

Tryckfrihetsförordningen är därför inte tillämplig för privata användarorganisationer. Dessa bör dock beakta att ett meddelande som sänds till en myndighet blir en inkommen handling hos myndigheten.

3.2 Illustration

Figur 3 illustrerar när en handling kan anses vara expedierad respektive inkommen vid kommunikation via SDK.



Figur 3 – När en handling kan anses vara expedierad respektive inkommen i SDK

Handlingen är krypterad och accesspunkterna (C2/C3) kan inte med rimliga medel kan ta del av den under överföringen.

Motivering till att handlingen kan anses vara expedierad hos användarorganisation A (sändare) när den är tillgänglig att ta del av i B:s meddelandetjänst, är att vi har ett kvitteringssystem inbyggt i SDK och att kontrollen över avsänd handling kvarligger hos avsändande myndighet till dess att den kvitterats hos mottagande myndighet och är tillgänglig hos mottagarens (B) meddelandetjänst. Sker ingen kvittens, dvs. avsändande myndighet (A) får ett felmeddelande, så innebär det att ingen handling har expedierats.

Med denna tolkning undviker avsändande myndighet situationen att om den elektroniska handlingen skulle anses expedierad när den lämnar avsändande myndighets accesspunkt men inte kommer fram till mottagaren att den ändå utgör en allmän handling som kan begäras ut.

Motivering till att handlingen kan anses vara inkommen hos användarorganisation B (mottagare), är att den är kvitterad och tillgänglig att ta del av i B:s meddelandetjänst.

Det är dock upp till varje användarorganisation att göra en egen bedömning.

4. Referenser

[1] Ineras tjänsten Säker digital kommunikations öppna informationsyta
https://inera.atlassian.net/wiki/spaces/OISDK/pages/2710601964/Informationss+kerhet

[2] Ineras ordlista - Ordlistan innehåller beskrivning av begrepp som används inom eller har beröringspunkter med Säker digital kommunikation. Länk till ordlistan

[3] Tryckfrihetsförordning (1949:105)
https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/tryckfrihetsforordning-1949105_sfs-1949-105